MEI-101
PF20J971/1-US

Title of the Invention

EMERGENCY ACCESS INTERCEPTION ACCORDING TO BLACK LIST

Inventors

Yohsuke ISHII,

Koji SONODA,

Masaaki IWASAKI.

EMERGENCY ACCESS INTERCEPTION ACCORDING TO BLACK LIST

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] This invention relates to an access control to information resources stored in a computer.

2. Description of the Related Art

[0002] Access control lists (ACLs) record permitted users for information resources stored in computers and are referred to restrict accesses by improper users, thereby enhancing securities for the information resources. Recently, a widely distributed environment, in which a plurality of networks are connected through a wide area network, such as the Internet, and enables the information resources including data files to be shared among the networks, is utilized. The ACL is also effective under the environment to enhance the securities. Under the environment, the ACLs, each of them being managed by each access controller connected with each network, are synchronized among all access controllers.

[0003] Since access right or permission to information resources are not stable but flexible, some cases require an interception of all accesses by a specific user under the widely distributed environment. JP 1999-282805A discloses a technique that synchronizes update of all ACLs in such a case where the access right of the specific user has to be prohibited, thereby intercepting all accesses by the prohibited user. Another technique periodically transmits a certification issued by a certificate authority for the access right, thereby intercepting accesses by users with invalid certifications.

[0004] But these conventional technique are not effective enough for emergency access interception in the following exemplified cases: a prohibition of access right after dismissing a specific user and detection of improper access. That is because the first technique requires long time to update the ACL, and the second technique cannot intercept the access before the new certification is issued and the old one turns to be expired.

[0005] The above-mentioned problem is not specific for the widely distributed environment but common to any system in which a plurality of access controllers cooperate together in controlling accesses to information resources.

SUMMARY OF THE INVENTION

[0006] To solve at least a part of the above-mentioned problem, this invention is directed to a first embodiment as follows. The first embodiment provides an access controller that controls an access to an information resource stored in a storage device, under an environment where a plurality of the access controllers and the storage devices are connected with a network. The access controller comprises an access restriction module, an access interception module, an input module and a list update module. The access restriction module is configured to restrict access to each information resource according to an access control list (ACL) on which access right to each information resource is recorded. The access interception module is configured to intercept an access by an access prohibited user listed on an access prohibition list. The input module is configured to receive user information of the access prohibited user. The list update module is configured to update the access prohibition list referred by each of the access controllers connected with the network, according to the user information input through the input

module.

[0007] Various information that can specify the access prohibited user is utilized as the user information, and may include, for example, user ID and a user name. Information to specify user's terminal or computer is also available as the user information. The ACL may contain detailed information of access right, such as "reading only" and "delete prohibited" or simple information, such as "access permitted" and "access prohibited".

[0008] The input module may receive the user information in various manners: receiving input of the information directly through user's keyboard operations or the like; reading out the information from data files recording the access prohibited users thereon; and receiving the access prohibition list itself. The list update module may update the access prohibition list through rewriting the user information registered in the list or replacing the access prohibition list itself.

[0009] This invention notifies all access controllers connected with the network of the user information for the emergency access interception, thereby enabling required emergency access interception under the widely distributed environment where a plurality of networks are connected each other through a wide area network, such as the Internet. The access prohibition list, which does not record access permission to each file but contains prohibited user information, is smaller than the ACL, which record access right corresponding to each information resource and has a large amount of data size. This smaller data size of the access prohibition list can reduce required time and load to update itself.

[0010] In the first embodiment, the list update module may send out an other access controller a registration instruction to register the input user information on the access prohibition list of the

other access controller. This application preferably reduces network traffic.

[0011] In the first embodiment, the list update module may send out a updated access prohibition list to an other access controller. The other access controller can easily replace the old list with the updated list.

[0012] A second embodiment of the invention provides an access controller that controls an access to an information resource stored in a storage device, under an environment where a plurality of the access controllers and the storage devices are connected with a network. The access controller comprises an access restriction module, a receiving module, a list update module and an access interception module. The access restriction module is configured to restrict access to each information resource according to an access control list on which access right to each information resource is recorded. The receiving module is configured to receive user information of an access prohibited user from the other access controller. The list update module is configured to update an access prohibition list, which records user information of access prohibited users, according to the received user information. The access interception module is configured to restrict the access by reference to the access prohibition list prior to the access control list.

[0013] In the second embodiment, each of the access controllers can reflect the access prohibited users information added to the access prohibition list of any other access controller to own access prohibition list without delay. Accordingly, the second embodiment effectively actualize the emergency access interception under the widely distributed environment.

[0014] Both in the first and second embodiments, the access interception module may also intercept the access that has not been

completed. This embodiment can intercept accesses that are started before updating the access prohibition list, accesses after the updating and accesses in waiting for processing, thereby enhancing the securities.

[0015] The access controller may further comprises an access control list update module configured to update the ACL according to the access prohibition list. This embodiment can automatically update the ACL to reduce maintenance load for the ACL.

[0016] The list update module may delete the user information on the access prohibition list at a predetermined timing.

[0017] Keeping the user information which has been once registered on the access prohibition list causes enlarged data size of the access prohibition list and requires longer time to check through the access prohibition list. Deleting the user information registered on the access prohibition list after updating the ACL as described above avoids enlarged size of the access prohibition list and the delay of the access interception process. Deleting the access prohibition list itself is also available.

[0018] The predetermined timing may be after the completion of updating the access control list. This allows each access controller connected with each network to individually delete the user information that has been reflected to the ACL. The access controller refers to the access prohibition list prior to the ACL, so that the load for checking the list can be reduced by deleting the user information from the access prohibition list.

[0019] The predetermined timing may be after all of the access control lists have been updated.

[0020] This embodiment ensures synchronization of access prohibition lists and ACLs among all of the access controllers. This embodiment can be especially effective in case where, for example,

the updated access prohibition list is distributed and replaced to old lists as the updating process. This embodiment ensures reflection of the updated access prohibition list to the ACL without lack due to provision of the list which has not been updated in those in some access controllers. Accordingly, the access interception according to the synchronized ACLs free from the above-mentioned lack can be actualized.

[0021] This invention may also provide an access control system by means of combination of the first and second embodiments. In the case where the access prohibition list of any one of access controllers is updated according to user information, the access controller sends out the user information or the updated access prohibition list to one or plural other access controllers in response to the update. The other access controller receives the user information or the updated access prohibition list to update own access prohibition list.

[0022] Transmitting the user information can reduce the traffic of the network, thereby enhancing the processing efficiency. On the other hand, transmitting the access prohibition list can inform the user information to specify a plurality of users to be subjected to the emergency access interception, and reduce the load for updating the access prohibition list in the receiving access controller by replacing it with the transmitted one.

[0023] The distribution module may broadcast the user information or the updated access prohibition list over all of other access controllers. This can make a simultaneous notice to all of the access controllers and ensure a synchronization of access prohibition lists.

[0024] The distribution module of each access controller may send out the user information or the updated prohibition list to

predetermined another access controller, thereby transmitting the user information or the updated prohibition list from one access controller to another. This can reduce required time for each transmission by reflecting hopping number on the network to selection of the destination access controller.

[0025] Various modifications are considerable for this invention out of the access controller and the access control system above, such as an access control method, a computer program to execute such access control, and a computer readable recording medium or a wave form in which the computer program is recorded or transmitted. Various features above are available each of these modifications.

[0026] When the present invention is configured as a computer program, a recording medium with such program recorded therein, or the like, such configuration may include an entire program for controlling or only a part that realizes the functions according to the present invention. A variety of computer-readable recording media may be used as the recording medium, including as flexible disk, CD-ROM, DVD-ROM, punched card, print with barcodes or other codes printed thereon, and internal storage device (memory such as ROM and RAM) and external storage device of the computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] Fig. 1 is a schematic that shows a system configuration of the embodiment.

[0028] Fig. 2 is a schematic that shows functional blocks in the access controller of the embodiment.

[0029] Fig. 3A and 3B are schematics that show an exemplar of the access control list.

[0030] Fig. 4 is a schematic that shows an exemplar of the black list.

[0031] Fig. 5 is a flowchart of the access control process.

[0032] Fig. 6 is a flowchart of the access control process in the access controller.

[0033] Fig. 7 is a flowchart of the black list distribution process.

[0034] Fig. 8 is a flowchart of the access interception process.

[0035] Fig. 9 is a flowchart of the ACL update process.

[0036] Fig. 10 is a flowchart of process for deleting the black list.

[0037] Fig. 11 is a schematic that shows a modified system configuration.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0038] The embodiments of this invention are described below.

A. Embodiment

A1. System Configuration

Fig. 1 is a schematic that shows a system configuration of the embodiment. An access control system 1000 is configured by connecting four networks A, B, C, D via an Internet INT. Connected with the network A via a local area network LAN1 are an access controller 100, a storage device 500, a client CL1 and the like. Similarly, connected with the networks B, C, D via local area networks LAN2, LAN3, LAN4 are access controllers 200, 300, 400, storage devices 600, 700, 800 and clients CL2, CL3, CL4, respectively.

[0039] Storage devices store data file 501, 601, 701, 801 and the like, respectively. The access control system 1000 is configured

as so-called widely distributed environment via the Internet INT. Each client can access not only to the storage device connected with own network, but also to others connected with other networks, and can read data files stored in these storage devices. For example, the client CL1 can read not only data file 501 in the storage device 500 but also data file 701 in the storage 700 on the network C.

[0040] Access right is required to access to every data file in these storage devices. Each access controller judges whether or not the access right is proper to control the access. Concretely, in the case where the client CL1 sends out an access request for the data file 501, the access controller 100 authenticates whether or not the client CL1's user is permitted to access to the data file 501 and controls the access according to the result of the authentication.

[0041] The access controller 100 manages two kinds of lists, an access control list 110 (hereinafter referred to as "ACL 110") and an access prohibition list 120 (hereinafter referred to as "black list 120"). The ACL 110 contains the detail access right to each object, such as a data file for each user. The black list 120 contains user information to specify users to be subjected to an emergency access interception. The access controller 100 first checks whether or not the user information of the requesting user is recorded on the black list 120, in response to an access requirement, and subsequently checks the ACL 110 if the user information is not recorded in the black list 120.

[0042] In the case where an emergency access interception is required in the network A, for example, the case where any one of users is dismissed, the access controller 100 also updates own black list 120 according to user information that is input through administrator's operation, and instructs other access controllers 200, 300, 400 to register this user information to the black list 220, 320, 420. The access controllers 200, 300, 400 receive this registration

instruction and update respective black list 220, 320, 420. This sequence effectively actualizes emergency access interception within all networks under the widely distributed environment.

A2. Functional Blocks

[0043] Fig. 2 is a schematic that shows functional blocks in the access controller of the embodiment. The access controller 100 includes a main controller 101, a communication controller 102, an ACL manager 103, a black list manager 104, an access manager 105, an input module 108 and a storage manager 109. The access manager 105 includes an access restriction module 106 and an access interception module 107 therein. The communication controller 102 controls following communications via the network: a communication with other devices in the own local area network LAN1, and a communication with other networks via the Internet INT.

[0044] The ACL manager 103 manages the ACL 110. The detail of the ACL 110 is described below. The black list manager 104 manages the black list 120. The user information to be registered includes user ID and user name, which are input by the administrator through the input module 108. The detail of the black list 120 is described below. The ACL manager 103 also updates ACL 110 by reflecting the user information of the black list 120 to the ACL 110. The access controller 100 deletes the user information which has been reflected to the ACL 110 from the black list 120, to ensure the processing efficiency of the access control.

[0045] The storage manager 109 manages storage devices in own local area network LAN1, such as storage device 500. The manage is for data in the storage devices and users accessing to each storage device by an access management table 109a illustrated in the figure.

[0046] The access management table 109a includes information such as: unique access ID of each access, access required object's name, statuses of access, and accessing user's information. In the illustrated example, the object"O-9" in the access ID [1] is in "Accessing" status by the user "S-3". Similarly, the object"O-7" in the access ID [2] is in "Access Waiting" status by the user "S-8".

[0047] The access manager 105 provides a function of access controls, including an access restriction according to the ACL and an emergency access interception. The access restriction module 106, included in the access manager 105, checks the ACL 110 for the authentication of user's access right and responses the result to the storage device 500, in response to an authentication requirement. The access interception module 107, also included in the access manager 105, checks the black list 120 to find the user in formation in the access management table 109a and if found, intercepts any access by the corresponding user, regardless of the status of access. In the illustrated example, finding the user "S-1" in the black list 120 causes the interception of all accesses from access IDs [3] and [6].

[0048] Fig. 3A is a schematics that shows an exemplar of the ACL. The ACL 110 includes information such as: unique ID of each access right, object's name, name of the user managing the object, permitted group, and permission of the access right. Fig. 3B shows general concept of the group. A group "G-1" in the dotted box includes users "S-1", "S-2", "S-3", "S-4", and "S-5." And a group "G-2" in the chained box is a part of the group "G-1" and includes users "S-1", "S-2", and "S-5." Accordingly, the users "S-1", "S-2", and "S-5" belong to both groups "G-1" and "G-2."

[0049] Respective characters, “R” and “W” in the "permission" represent "Read" or readable and "Write" or writable. Concretely, the

object [O-1] in the ID [1] is permitted "R, W", which means the object is both readable and writable by the user "S-3". Similarly, the object [O-1] in the ID [2] is permitted "R", which means the object is further readable by users in the group "G-1."

[0050] Fig. 4 is a schematic that shows an exemplar of the black list. The black list 120 includes user information, such as user ID and user name. Alternatively, either the user ID or the user name may be omitted. In Fig. 4, the user information, the user ID "S-1" and the user name "Taro Hitachi", is recorded in the black list 120, which is recorded by the access controller 100 in response to an access interception requirement. The black list 120 can contain a plurality of users at one time. And a new user to be subjected to the emergency access interception can be added to the black list.

[0051] Other access controllers 200, 300, and 400 have similar configuration, and the explanation for them is omitted.

A3. Access Control Process

[0052] Fig. 5 is a flowchart of the access control process, which enables the client CL1 to access the data file 501 in the storage device 500.

[0053] The client CL1 sends out an access requirement to the access controller 100 (step Sa100). The access controller 100 receives the requirement and authenticates the access right of the user by checking the black list 120 and the ACL 110. The access controller 100 accesses to the storage 500 according to the authentication result (step Sa102) and responses the access result to the client CL1 (step Sa103, Sa104).

[0054] Fig. 6 is a flowchart of the access control process in the access controller, which corresponds to step Sa101 in Fig. 5 and is executed by the access controller 100.

[0055] The access controller 100 receives the request for authentication of access right to the storage device 500 from the client CL1, and also receives user ID and access-required object's name (step S10). Then the access controller 100 checks the black list 120 (step S11) to judge whether or not the accessing user is registered in the list 120 (step S12). If registered, the access controller 100 sends out the storage device 500 an access prohibition notice (step S16) to intercept all accesses by the user.

[0056] If not registered, the access controller 100 then checks the ACL 110 to find the permission for the access-required object (step S13). If permitted (step S14), the access controller 100 accesses to the storage device 500 under the permission, such as readable and writable (step S15). If not permitted (step S14), though the user is out of the black list 120, the access controller 100 sends out the access prohibition notice to the storage device 500 (step S16).

A4. Black List Distribution Process

[0057] Fig. 7 is a flowchart of the black list distribution process. When receiving input of the access interception requirement through the administrator's operation, the access controller 100 registers the user information that is subjected to be the access interception on own black list 120 and broadcasts the user information and registration instruction of the information to the access controllers 200, 300, 400. Fig. 7 exemplifies one case in which the access controller 100 transmits the instruction to the access controller 200.

[0058] According to the flowchart of Fig. 7, the access controller 100 inputs the access interception requirement through the administrator's operation (step S20) and registers the user information including user ID and user's name in the black list 120 (step S21).

The access controller 100 then transmits the registration instruction and the user information to the access controller 200 as well as the access controller 300 and 400 to instruct each access controller to register the user information in its own black list (step S22).

[0059] Subsequently, the access controller 100 executes the access interception process to intercept any access by the user listed on the black list, as described below (step S23). The access controller 100 updates the ACL according to the black list (step S24), as described below, and deletes the user information from the black list 120 (step S25) after the updating.

[0060] The access controller 200 receives the registration instruction transmitted from the access controller 100 at step S22 and updates the black list 220 by adding the user information, user ID and user's name to the list 220 (step S31). The access controller 200 executes the access interception process according to the updated list 220 (step S32), updates the ACL (step S33), and deletes the user information from the black list 220 (step S34). The processes of steps S32 - S34 are similar to those of steps S23 - S25 in the access controller 100. The access interception process (step S23, step S32) and the process to update the ACL (step S24, step S33) are described below.

A5.access interception process

[0061] Fig. 8 is a flowchart of the access interception process. This process corresponds to the processes of steps S23 and S32 in Fig. 7 and is executed by the access controllers 100 and 200.

[0062] The access controller 100 refers to the black list 120 and the access management table 109a (step S40, S41) to define statuses of accesses by black listed user, that is, to determine whether or not there is any black listed user's access in the status of

"accessing" or "access waiting" (step S42). In the case where such an access is found, the access controller 100 intercepts all accesses by the black listed user regardless of the status, "accessing" or "access waiting" (step S43). On the other hand, in the case where no access by the black listed user is found, the access controller 100 returns from this process.

A6. ACL Update Process

[0063] Fig. 9 is a flowchart of the ACL update process. This process corresponds to the process of steps S24 and S33 in Fig. 7 and is executed by the access controllers 100 and 200. The user with User ID "S-1" and user name "Taro Hitachi" is assumed to be a subject of the access interception.

[0064] The access controller 100 refers to the black list 120 and the ACL 110 (step S50) to delete the user ID "S-1" from a group, thereby updating the group setting (step S51). The access controller 100 subsequently retrieves all records with user ID "S-1" from the ACL 110 and deletes them (step S52). Concretely, the record ID [5] is shown to be deleted in the Fig. 7.

[0065] This process enables the ACL 110 relating to the user ID "S-1" to be updated with the group setting kept.

[0066] The embodiment described above can response situations where access right of some users must be prohibited without delay, and can transmit the user information of such users to all access controllers under the widely distributed environment. Each access controller can enhance securities by utilizing the black list prior to the ACL, because updating the ACL needs longer time and is suitable for an emergency access interception.

B. Modifications

[0067] This invention is not limited to the above embodiment but there may be various modifications within the spirit thereof.

B1. First Modification

[0068] Unlike the embodiment in which the access controller 100 transmits the user information and the registration instruction to all other access controllers, the access controller 100 may transmit the updated black list in place of the information. This ensures effective updating of the black list in the other access controllers.

[0069] Unlike the embodiment in which the access controller deletes the user information from the black list after updating the ACL, the access controller may delete the old black list in response to receipt of the updated black list. Fig. 10 is a flowchart of process for deleting the black list. The updating of the ACL is assumed to be completed before the process.

[0070] According to the process of Fig. 10, the completion of updating the ACL (step Sa200) causes the access controller 200 to notify the access controller 100 of the completion to the distributor of the black list, (step Sa201). Similarly, the access controllers 300 and 400 notify the completion (step Sa202 - step Sa205).

[0071] After receiving the notification from all other access controllers, the access controller 100 deletes own black list (step Sa207) and instruct other access controllers to delete their black lists. In response to this instruction, the access controllers 200, 300, and 400 delete their own black lists (steps Sa208 - Sa213).

[0072] This modification ensures the synchronization of the ACL in all access controllers. This modification ensures reflection of all user information in the black list to the ACL, even when a plurality of access interception requirements are submitted in s short period and causes frequent updates of the black list.

B2. Second Modification

[0073] Unlike the embodiment in which the access controller 100 simultaneously transmits the updated black list to all other access controllers 200, 300 and 400, the access controller may transmit the list to one of the other access controllers as shown in Fig. 11. The receiving controller can transmit the list to another. As illustrated with bold arrows in Fig. 11, the access controller 100 transmits the black list to the access controller 200, the controller 200 to the controller 300, and the controller 300 to the controller 400. The destination of the transmission can be selected in consideration of the number of hopping on the networks, and thus enhances efficiency of the transmission.

B3. Third Modification

[0074] The embodiment can apply a certificate authority that manages certifications of proper users under widely distributed environment. In this system, the certificate authority may execute the access control with the black list prior to authenticate the certification, which ensures securities.